Notice of Allowability	Application No.	Applicant(s)	
	09/672,496	BRICKELL ET AL.	
	Examiner	Art Unit	
	Jacob F. Betit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed on 3 February 2005*.

2. ☒ The allowed claim(s) is/are *29-38,40,41 and 43*.

3. ☒ The drawings filed on *16 March 2001 (figures 1-2 and 4-5) and 18 June 2004 (figure 3)* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20050228* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

SAM RIMELL
PRIMARY EXAMINER

DETAILED ACTION

Remarks

1. In response to communications filed on 3-February-2005, claims 30, 33, 38, and 41 are currently amended and claims 39 and 42 are cancelled per applicants request. Claims 29-38, 40-41, and 43 are presently pending in the application.

2. In view of the examiner's amendment, authorized by the attorney of record, claims 38 and 41 are amended. Claims 29-38, 40-41, and 43 are pending in the application.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Roger R. Wise on 01-March-2005 (see enclosed interview summary for details).

The application has been amended as follows. This listing of claims will replace all prior versions of the claims in the application.

Claims 1-28 (cancelled).

29. (currently amended) A method of generating and transmitting a private encryption key, comprising:

generating a public encryption key and a private encryption key at a client system;

inputting a password and generating a random number;

creating a random private key by exclusive-ORing the private key with the random number;

generating a first hash value by hashing the password, a username, and a constant value;

encrypting the random private key using the first hash value as an encryption key to create an encrypted random key;

generating a second hash value by hashing the password, the username, and a second constant value; and

transmitting the username, the second hash value, and the encrypted random key to a sever for storage.

30. (previously presented) The method of claim 29, further including further authenticating a user at the server.

31. (previously presented) The method of claim 30, wherein the method of authenticating is using a biometric device.

32. (previously presented) The method of claim 29, further including deleting the private encryption key from the client system.

33. (previously presented) The method of claim 29, further including deleting the constant value from the client system.

34. (previously presented) A computer readable medium containing instructions for execution by a processor, the instructions, which when executed, cause the processor to:

generate a public encryption key and a private encryption key at a client system, which includes the processor;

receive a password and generate a random number;

create a random private key by exclusive-ORing the private key with the random number;

generate a first hash value by hashing the password, a username, and a constant value;

encrypt the random private key using the first hash value as an encryption key to create an encrypted random key;

generate a second hash value by hashing the password, the username, and a second constant value; and

transmit the username, the second hash value, and the encrypted random key to a server for storage.

35. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the private encryption key from the client system.

36. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the constant value.

37. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the second constant value.

38. (currently amended) A method for retrieving a stored password, comprising:

receiving a password and a username;

generating a first hash value using the password, the username, and a first constant value;

generating a second hash value using the password, the username, and a second constant value;

transmitting the second hash value and the username to a key server;

receiving an encrypted random private key from the key server ~~if~~ when the username and the second hash value match a stored username value and a stored hash value; and

decrypting the encrypted random private key using the first ~~has~~ hash value as an encryption key to ~~generating~~ generate a random private key.

Claim 39 (cancelled).

40. (previously presented) The method of claim 38, further including exclusive-ORing a random number with the random private key to generate a private key.

41. (currently amended) A computer readable medium containing instructions for execution by a processor, the instructions, which when executed, cause the processor to:

receive a password and a username;

generate a first hash value using the password, the username, and a first constant value;

generate a second hash value using the password, the username, and a second constant value;

transmit the second hash value and the username to a key server;

receive an encrypted random private key from the key server ~~if~~ when the username and the second hash value match a stored username value and a stored hash value; and

decrypt the encrypted random private key using the first hash value as an encryption key to generate a random private key.

Claim 42 (cancelled).

43. (previously presented) The computer-readable medium of claim 41, including instructions, which when executed causes the processor to exclusive-OR a random number with the random private key to generate a private key.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance:

The prior art of record does not disclose, teach, or suggest the claimed limitations (in combination with all other features of the claim):

generating a first hash value by hashing the password, a username, and a constant value;

encrypting the random private key using the first hash value as an encryption key to create an encrypted random key;

generating a second hash value by hashing the password, the username, and a second constant value; and

transmitting the username, the second hash value, and the encrypted random key to a server for storage as claimed in claim 29.

The prior art of record does not disclose, teach, or suggest the claimed limitations (in combination with all other features of the claim):

generate a first hash value by hashing the password, a username, and a constant value;

encrypt the random private key using the first hash value as an encryption key to create an encrypted random key;

generate a second hash value by hashing the password, the username, and a second constant value; and

transmit the username, the second hash value, and the encrypted random key to a server for storage as claimed in claim 34.

The prior art of record does not disclose, teach, or suggest the claimed limitations (in combination with all other features of the claim):

generating a first hash value using the password, the username, and a first constant value;

generating a second hash value using the password, the username, and a second constant value;

transmitting the second hash value and the username to a key server;

receiving an encrypted random private key from the key server when the username and the second hash value match a stored username value and a stored hash value; and

decrypting the encrypted random private key using the first hash value as an encryption key to generate a random private key as claimed in claim 38.

The prior art of record does not disclose, teach, or suggest the claimed limitations (in combination with all other features of the claim):

generate a first hash value using the password, the username, and a first constant value;

generate a second hash value using the password, the username, and a second constant value;

transmit the second hash value and the username to a key server;

receive an encrypted random private key from the key server when the username and the second hash value match a stored username value and a stored hash value; and

decrypt the encrypted random private key using the first hash value as an encryption key to generating a random private key as claimed in claim 41.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

U.S. patent No. 6,230,269 B1 to Spies et al. for teaching construction of a public/private key pair from key source material, the user ID, and the user password.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-4075. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (571) 272-4083. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
28 Feb 2005

SAM RIMELL
PRIMARY EXAMINER